SELVEJE DANMARKS

VEJLEDNING OM HÅNDTERING AF EKSTERN PERSONDATA

SELVEJE DANMARK

Brancheforeningen for
selvejende organisationer

INDHOLD

1 TJEKLISTE

ELLER NOGEN AF DE SPØRGSMÅL MAN SOM ORGANISATION KAN STILLE SIG SELV.

Databehandler eller dataansvarlig? (se afsnit 6)

Kortlægning over den data der behandles: Oplysninger om borgere, om ansatte, tidligere visiterede borgere og ansatte, pårørende mv. (se afsnit 4.3)

Beskrivelse af hvem i organisationens omverden, der vil kunne være modtagere af oplysninger, herunder en kortlægning af organisationens omverden (se afsnit 5)

Beskrivelse af med hvilken hjemmel oplysningerne behandles. Er der tale om lovhjemmel, er andre kriterier opfyldt, eller kræves borgerens samtykke? (afsnit 4.3)

Beskrivelse af hvor længe forskellige oplysninger skal opbevares (er der specifikke lovkrav, forældelsesregler, mv.) (se afsnit 10)

Vurdering af behovet for en DPO (se afsnit 7)

Bruger organisationer underleverandører til at hjælpe med behandling af data, skal der laves databehandleraftaler f.eks. hvis lønadministration er udliciteret (se standard for denne på www.danskerhverv.dk eller kontakt den pågældende leverandør).

Vurdering af behovet for udarbejdelse af en fortegnelse – og den konkrete udarbejdelse af fortegnelsen (se afsnit 9).

Hvordan anvender vi e-mails til kommunikation af personoplysninger? (se afsnit 5.1.3)

Vurdering af hvilken betydning kravet om god databehandlerskik (se afsnit 4.2) **har for organisationen og eventuel udarbejdelse af de nødvendige informationer og/eller samtykkeerklæringer, der skal anvendes.**

Instruktion af alle medarbejdere i hvordan data skal behandles i organisationen.

Udarbejdelse en persondatapolitik (bilag 2)

2 OM VEJLEDNINGEN

Vejledningen er udarbejdet af Dansk Erhverv og Selveje Danmark, og den gennemgår en række af de mange situationer, hvor en organisation behandler eksterne persondata, det vil sige oplysninger om privatpersoner, der ikke er medarbejdere i organisationen som eksempelvis patienter, beboere og borgere.

Reglerne for behandling af personoplysninger og beskyttelse af persondata er under forandring. De eksisterende regler i blandt andet persondataloven erstattes af et nyt regelsæt fra den 25. maj 2018. Derfor indeholder denne vejledning både information om det eksisterende regelsæt og om de nye regler, i det omfang disse regler kendes. Se nærmere under afsnit 2.

Da vejledningen tager afsæt i de regler og vejledninger, vi aktuelt kender (1.marts 2018), og den praksis der er knyttet til de regler, så er det vigtigt, at du som organisation også fremover følger området, retter din praksis til og tilpasser jeres arbejde med persondata efter fremtidige regler, vejledninger og praksis. Reglerne stiller også en række krav, hvis data opbevares i andre lande, særligt hvis der er tale om lande udenfor EU, bl.a. til datasikkerhed i de pågældende lande. Det antages, at det ikke er relevant for de fleste selvejende organisationer, hvorfor dette aspekt ikke er omfattet af denne vejledning, men er det tilfældet, skal dette aspekt inddrages bl.a. i fortegnelsen og i de databehandleraftaler, der indgås.

Reglernes anvendelsesområde og systematik gennemgås kort i vejledningens afsnit 2 og 3. I de følgende afsnit er en gennemgang af en række konkrete situationer, hvor en organisation behandler personoplysninger om privatpersoner som eksempelvis patienter, beboere og borgere. Med vejledningen sættes fokus på en række overvejelser, som organisationen kan gøre sig allerede nu, inden det nye regelsæt skal anvendes, eksempelvis:

- Hvilke personoplysninger håndterer organisationen om eksempelvis patienter, beboere og borgere – både nuværende og tidligere – og hvordan håndteres de? Er der eventuelt forhold her, der skal rettes op, for at organisationen lever op til databeskyttelsesreglerne?
- Har organisationen en oversigt over behandlinger af personoplysninger om eksempelvis patienter, beboere og borgere?
- Overholder organisationen sikkerhedskravene i databeskyttelsesreglerne, eksempelvis i forhold til brug af eksterne leverandører?
- Skal organisationen have en databeskyttelsesrådgiver pr. 25. maj 2018?

Datatilsynet har udgivet en pjece med generel information om organisationens interne arbejde med databeskyttelsesreglerne: "Forberedelser forud for EU's databeskyttelsesforordning - 12 spørgsmål som dataansvarlige allerede nu med fordel kan forholde sig til". Pjecen kan hentes på tilsynets hjemmeside om de nye databeskyttelsesregler fra 25. maj 2018 – www.dbreform.dk.

På samme hjemmeside kan også findes de vejledninger, som Datatilsynet har udfærdiget i samarbejde med Erhvervsstyrelsen, Justitsministeriet og Digitaliseringsstyrelsen. Vejledningerne bidrager til en større forståelse af de kommende regler, og hvordan de skal fortolkes i Danmark. Dansk Erhverv har ligeledes udfærdiget en vejledning, der giver gode råd til virksomheders behandling af medarbejderdata.

Vejledningen kan findes på www.danskerhverv.dk. Dansk Erhvervs medlemmer kan også få konkret rådgivning om behandling af personoplysninger, se nærmere i afsnit 12.

3 NYE REGLER FRA 25. MAJ 2018

I dag reguleres en organisations registrering og brug af personoplysninger om eksempelvis, patienter, beboere og borgere som udgangspunkt af den danske persondatalov. Der er også særlig lovgivning på en række områder. Som eksempel kan nævnes lovgivningen om behandling af patienters sundhedsdata i eksempelvis sundhedsloven og bekendtgørelsen om information og samtykke og om videregivelse af helbredsoplysninger mv.
Der er i EU vedtaget et nyt regelsæt om persondatabeskyttelse, der skal anvendes fra 25. maj 2018 ("databeskyttelsesforordningen").[1] Dele af forordningen enten kan eller skal gennemføres ved supplerende lovgivning i Danmark. Frem-

[1] EUROPA-PARLAMENTET OG RÅDETS FORORDNING (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direkte 95/46/EF (generel forordning om databeskyttelse)

over vil reglerne om databeskyttelse både fremgå af databeskyttelsesforord-ningen, en ny dansk databeskyttelseslov og i dansk særlovgivning. Den supplerende danske lovgivning forventes vedtaget i løbet af efteråret 2017. Justitsministeriet vil løbende udsende en række vejledninger om regelsættets enkelte dele frem til foråret 2018, se yderligere under punkt 1.

Hvordan det samlede regelsæt i sidste ende kommer til at se ud, har betydning for en organisations muligheder for at behandle oplysninger om patienter, beboere og borgere, mv. i forskellige situationer fra den 25. maj 2018. Denne vejledning er skrevet ud fra den gældende persondatalov og praksis fra Datatilsynet mv. Samtidig er der under de enkelte emner tilføjet afsnit om reglerne fra 25. maj 2018 ud fra de kendte regler og fortolkningsbidrag[2] .

4 PERSONDATALOVENS SYSTEMATIK

4.1 Lovens Område

Formålet med loven er at beskytte oplysninger om fysiske personer og sikre databeskyttelse. Lovens almene karakter gør, at flere bestemmelser er meget generelt formuleret og kræver fortolkning, når reglerne skal anvendes på ekstern persondata, der behandles i og af organisationer.

Loven har et bredt anvendelsesområde og omfatter forskellige typer behandling af personoplysninger[3]:

1. Elektronisk behandling.
2. Ikke-elektronisk (manuel) behandling af personoplysninger, når oplysningerne er eller vil blive indeholdt i et register.
3. Anden ikke-elektronisk systematisk behandling der udføres for private. Her omfatter loven dog alene oplysninger om:
    a. Personernes private eller økonomiske forhold.
    b. Personlige forhold som med rimelighed kan forlanges unddraget offentligheden.

En ”behandling” skal forstås meget bredt og omfatter bl.a. indsamling, registrering, systematisering, opbevaring, søgning, videregivelse og sletning. Loven gælder således bredt for aktiviteter, som relaterer sig til personoplysninger.

Loven gælder f.eks. når organisationen:

- Noterer personoplysninger om en kunde, patient, beboer eller borger i et tekstbehandlingsprogram via en PC.
- Sender en e-mail med personoplysninger om en kunde, patient, beboer eller borger.
- Gemmer eksempelvis patientjournaler og andre personoplysninger på beboere og borgere i et it-system.
- Opbevarer oplysninger om patienter, beboere eller borgere i elektroniske sager, ringbind eller på anden systematisk vis.

Reglerne fra 25. maj 2018

Justitsministeriet lægger i udkastet til den nye danske databeskyttelseslov op til, at anden ikke-elektronisk systematisk behandling, som udføres for private (nr. 3 ovenfor) ikke længere skal være omfattet af regelsættet om persondata. Baggrunden er ifølge ministeriet, at denne bestemmelse i takt med den teknologiske udvikling har et meget begrænset anvendelsesområde.

4.2 Generelle ufravigelige principper

Loven indeholder en række grundlæggende principper, som altid skal overholdes ved behandlingen af personoplysninger. Det gælder således også, når en organisation behandler oplysninger om sine patienter, beboere eller borgere (”registrerede”).

Personoplysninger skal således altid behandles i overensstemmelse med god databehandlingsskik. Indholdet af dette generelle begreb fastsættes i praksis, men det dækker bl.a. over følgende:

- Indsamling af oplysninger skal ske til udtrykkeligt angivne og saglige formål. En senere behandling af oplysningerne må ikke være uforenelige med de(t) oprindelige formål. I praksis vil det være afgørende, om behandlingen sigter mod at løse opgaver, der ligger indenfor organisationens kompetence og varetager en anerkendelsesværdig interesse. Der skal være tale om en interesse og et eller flere formål, som organisationen har defineret og kan kommunikere til sine patienter, beboere eller borgere.

[2] Den nye databeskyttelsesforordning, betænkning om denne forordning fra Justitsministeriet og udkast til den danske supplerende databeskyttelseslov fra Justitsministeriet, som har været i høring over sommeren 2017, og blev fremsat af justitsministeren den 25. oktober 2017 og skal i første behandling i Folketinget den 16. november 2017.

[3] Notatet gennemgå ikke de situationer, hvor de gældende og/eller kommende regler omfatter virksomheder etableret uden for Danmark, internationale dataoverførsler mv. Kontakt Dansk Erhverv, hvis I har brug for rådgivning herom.

- Oplysninger, der behandles, skal være relevante og tilstrækkelige, og må ikke omfatte mere, end hvad opfyldelse af formålet med behandlingen kræver. Heri ligger en proportionalitetsvurdering, som organisationer løbende skal foretage i deres behandling af personoplysninger.
- Endelig skal behandling af personoplysninger ske således, at der sker den fornødne ajourføring af oplysningerne, ligesom der skal føres fornøden kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger.

Principperne om opbevaring omtales særskilt i afsnit 10.

Reglerne fra 25. maj 2018
Persondataforordningen indeholder også en række generelle principper, som altid skal overholdes ved behandlingen af personoplysninger. Justitsministeriet vurderer, at der hovedsageligt er tale om en videreførelse af de gældende principper i persondataloven, selvom formuleringerne ikke på alle punkter er ens. Samtidig skal en organisation kunne bevise, at principperne overholdes, se også afsnit 9.

4.3 Muligheder for at behandle personoplysninger

4.3.1 Typer af oplysninger
En personoplysning er enhver form for information om en identificeret eller identificerbar person. Persondataloven opdeler personoplysninger i tre typer af oplysninger:

1. Følsomme oplysninger, se afsnit 4.3.2.
2. Semi-følsomme (oplysninger om rent private forhold), se afsnit 4.3.3.
3. Almindelige oplysninger, se afsnit 4.3.4.

Der er også særlige regler om personnummer, se afsnit 5.

Loven indeholder efter samme opdeling forskellige betingelser for, hvornår de enkelte kategorier af oplysninger kan behandles.

4.3.2 Følsomme oplysninger
Følsomme oplysninger er oplysninger om:

- Racemæssig eller etnisk baggrund.
- Politisk, religiøs eller filosofisk overbevisning.
- Fagforeningsmæssige tilhørsforhold.
- Oplysning om helbredsforhold.
- Oplysninger om seksuelle forhold.

Adgangen til at behandle følsomme personoplysninger er relativt snæver. En organisation kan behandle følsomme oplysninger, hvis:

- Der er hjemmel til behandlingen i anden lovgivning f.eks. i lov om socialtilsyn eller bekendtgørelse om autoriserede sundhedspersoners patientjournaler. Det vil sige i alle de situationer, hvor organisationen er pålagt at behandle oplysninger eller pålagt at kunne give oplysningerne til f.eks. et offentligt tilsyn.
- Den registrerede har givet sit udtrykkelige samtykke til det.
- Behandlingen er nødvendig for at beskytte den registreredes eller en anden persons vitale interesser i tilfælde, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke.
- I visse tilfælde hvis oplysningerne er offentliggjort af den registrerede selv.
- Behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

Helbredsmæssige forhold dækker eksempelvis over oplysninger om en persons tidligere, nuværende og fremtidige fysiske eller psykiske tilstand samt oplysninger om medicinbrug, misbrug af narkotika, alkohol og lignende.

En række regler på velfærdsområdet betyder, at de organisationer, der arbejder med mennesker som f.eks. plejehjem, døgninstitutioner, bosteder og opholdstilbud efter servicelovens §§ 66, 107 og 108, vil skulle samle og behandle følsom-

me oplysninger om helbred, seksuel orientering, diagnoser mv. i elektroniske dagbøger, patientjournaler, mv. Er der hjemmel til opsamling af de specifikke følsomme oplysninger, så vil der ikke være krav om, at der skal gives et samtykke, men den berørte borger skal iht. princippet om god databehandlingsskik informeres om hvilke oplysninger, der samles, og om at vedkommende kan få indsigt i disse.

Et eksempel fra det sociale område: Af lov om socialtilsyn § 20, fremgår følgende: "Videregivelse af oplysninger fra et tilbud som nævnt i § 4, stk. 1, til socialtilsynet kan ske uden samtykke fra borgeren, når videregivelsen er nødvendig for udførelsen af det driftsorienterede tilsyn".

Tilsynets arbejde sker i overensstemmelse med den kvalitetsmodel, der er optrykt som bilag til bekendtgørelse om socialtilsynet. Af den fremgår det, at socialtilsynet bl.a. vil have fokus på følgende forhold, som lægges til grund for tilsynets vurdering af kvaliteten, forhold som alle på den ene eller anden måde vil kunne betyde, at der skal ske behandling af følsomme oplysninger:

Indikator 1.a:
Tilbuddet opstiller i samarbejde med borgerne konkrete, individuelle mål i forhold til at understøtte borgernes skolegang, uddannelse, beskæftigelse eller samværs- og aktivitetstilbud, og der følges op herpå.

Indikator 2.a:
Tilbuddet opstiller i samarbejde med borgerne konkrete, individuelle mål i forhold til at understøtte udvikling af borgernes kompetencer til at indgå i sociale relationer og leve et så selvstændigt liv som muligt, og der følges op herpå.

Indikator 2.f:
Børnene og/eller de unge har en fortrolig relation til en eller flere voksne, der har en positiv betydning for deres liv

Indikator 3.b:
Tilbuddet dokumenterer resultater med udgangspunkt i konkrete, klare mål for borgerne til løbende brug for egen læring og forbedring af indsatsen.

Indikator 3.c:
Tilbuddet opnår positive resultater i forhold til opfyldelsen af de mål, visiterende kommuner har opstillet for borgernes ophold.

Indikator 3.d:
Tilbuddet samarbejder aktivt med relevante eksterne aktører for at understøtte, at målene for borgerne opnås.

Indikator 5.b:
Borgerne har med støtte fra tilbuddet adgang til relevante sundhedsydelser.

Indikator 5.c:
Tilbuddets viden og indsats vedrørende borgernes fysiske og mentale sundhed modsvarer borgernes behov.

I det daglige arbejde vil der derfor være hjemmel til at samle de oplysninger, der er nødvendige, for at kunne leve op til de krav som tilsynet stiller. Husk dog, at det i alle tilfælde skal ske i overensstemmelse med god databehandlingsskik.

En stiftelse, en forening eller en anden almennyttig organisation, hvis sigte er af politisk, filosofisk, religiøs eller faglig art, kan inden for rammerne af sin organisation foretage behandling af følsomme oplysninger om organisationens medlem-

mer eller personer, der på grund af organisationens formål er i regelmæssig kontakt med den pågældende organisation. En videregivelse af disse følsomme personoplysninger til eksempelvis en anden organisation kan kun finde sted, hvis den registrerede har meddelt sit udtrykkelige samtykke til dette, eller der er en anden behandlingshjemmel til videregivelsen, se ovenstående liste. Derudover kan der også ske behandling af følsomme oplysninger, hvis behandlingen er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Hvis behandlingen af følsomme oplysninger sker af grunde, der vedrører hensynet til vigtige samfundsmæssige interesser, vil Datatilsynet endvidere kunne give tilladelse til denne behandling. Som eksempel kan nævnes behandling af personoplysninger hos Børns Vilkår, hvor Datatilsynet gav tilladelse til behandling af følsomme oplysninger i forbindelse med udsatte børn og unge, der henvender sig til Børns Vilkår, og hvor Børns Vilkår tilbyder støtte, rådgivning og bisidning til disse udsatte børn og unge.

4.3.3 Semi-følsomme oplysninger

Oplysninger om rent private forhold er oplysninger om:

- Strafbare forhold.
- Væsentlige sociale problemer.
- Andre rent private forhold, som ikke er nævnt under kategorien af følsomme oplysninger.

Semi-følsomme oplysninger må som udgangspunkt kun behandles og videregives af organisationen, hvis den registrerede har givet sit udtrykkelige samtykke. Samtykkekravet kan dog fraviges, hvis der er i lovgivningen er hjemmel til behandlingen, eller hvor behandling og videregivelse af personoplysningen er nødvendig for, at organisationen kan varetage en berettiget interesse, der klart overstiger hensynet til den registrerede, og videregivelsen sker til varetagelse af offentlige eller private interesser, der ligeledes klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.

Adgangen til at behandle oplysninger om rent private forhold uden den registreredes samtykke er særdeles snæver. Eksempelvis vil behandling uden samtykke kunne ske, hvis en organisation registrerer oplysninger om ophavsretskrænkelser (strafbare forhold) med henblik på at overveje, hvorvidt der skal ske indgivelse af politianmeldelse eller iværksættelse af privat påtale for overtrædelse af ophavsretslovgivningen. Behandlingen af semi-følsomme oplysninger vil endvidere kunne ske, hvis betingelserne for behandling af følsomme oplysninger er opfyldt.

4.3.4 Almindelige oplysninger

Adgangen til at behandle almindelige personoplysninger er væsentligt videre, end hvad der gælder for behandling af følsomme og semi-følsomme oplysninger.

Almindelige oplysninger kan behandles hvis:

- Der er hjemmel til behandlingen i anden lovgivning f.eks. i lov om socialtilsyn eller bekendtgørelse om autoriserede sundhedspersoners patientjournaler. Det vil sige i alle de situationer, hvor organisationen er pålagt at behandle oplysninger eller pålagt, at kunne give oplysningerne til f.eks. et offentligt tilsyn.
- Når den registrerede har givet sit udtrykkelige samtykke.
- Når behandlingen er nødvendig af hensyn til opfyldelse af en aftale, den registrerede er eller bliver part i.
- Når behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler organisationen som dataansvarlig.
- Når behandlingen er nødvendig for at beskytte den registreredes vitale interesser.
- Når behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse.
- Når behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som organisationen som dataansvarlig, eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt.
- Når det kan godtgøres, at behandlingen af oplysningerne er nødvendig for, at den dataansvarlige, eller den tredjemand, som oplysningerne er videregivet til, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse. Her skal der ske en konkret afvejning.

I et eksisterende kundeforhold vil organisationen f.eks. kunne behandle almindelige oplysninger på kunden som kundens navn, adresse og e-mail, da der er tale om behandling af kundens personoplysninger, som er nødvendige for, at organisationen kan opfylde sin aftale med kunden.

I forhold til socialpædagogisk arbejde og lignende, der udføres med hjemmel i serviceloven og f.eks. lov om aktiv beskæftigelsesindsats, vil der som alt overvejende hovedregel være tale om, at borgeren frivilligt vælger at indtræde i det pågældende forløb. Der er således ikke tale om tvang. I de situationer vil behandlingen af almindelige oplysninger kunne ske, når behandlingen er nødvendig af hensyn til opfyldelse af en aftale, den registrerede er eller bliver part i, og dermed at det tilbud, der arbejder med borgeren, ikke vil kunne gennemføre arbejdet, hvis der ikke kan ske en løbende opsamling og refleksion over f.eks. væsentlige sociale problemer, familieforhold, forhold omkring uddannelse og arbejde mv.

4.3.5 Særligt om samtykke
Som nævnt flere steder kan de forskellige typer af personoplysninger behandles, hvis organisationen har fået samtykke til det fra den registrerede.

Samtykke er et væsentligt element i databeskyttelsesretten. Alle former for oplysninger og alle former for behandling kan som udgangspunkt foretages, hvis der foreligger et gyldigt samtykke fra den registrerede. Der gælder som sådan ikke noget formkrav til et samtykke (f.eks. skriftlighed), men udgangspunktet er, at det skal være frivilligt, informeret og udtrykkeligt. Det er organisationens ansvar at kunne dokumentere, at der er givet samtykke.

Overvejelse: Det kan overvejes, at lade behandlingen af oplysninger om borgere visiteret til plejehjem, døgntilbud, bosted eller lignende begrunde i den direkte lovhjemmel fremfor et samtykke. Årsagen er, at samtykket kan trækkes tilbage, hvilket kan vanskeliggøre det videre arbejde og gøre det umuligt at leve op til kravene fra Socialtilsynet og/eller det risikobaserede tilsyn i Styrelsen for patientsikkerhed.

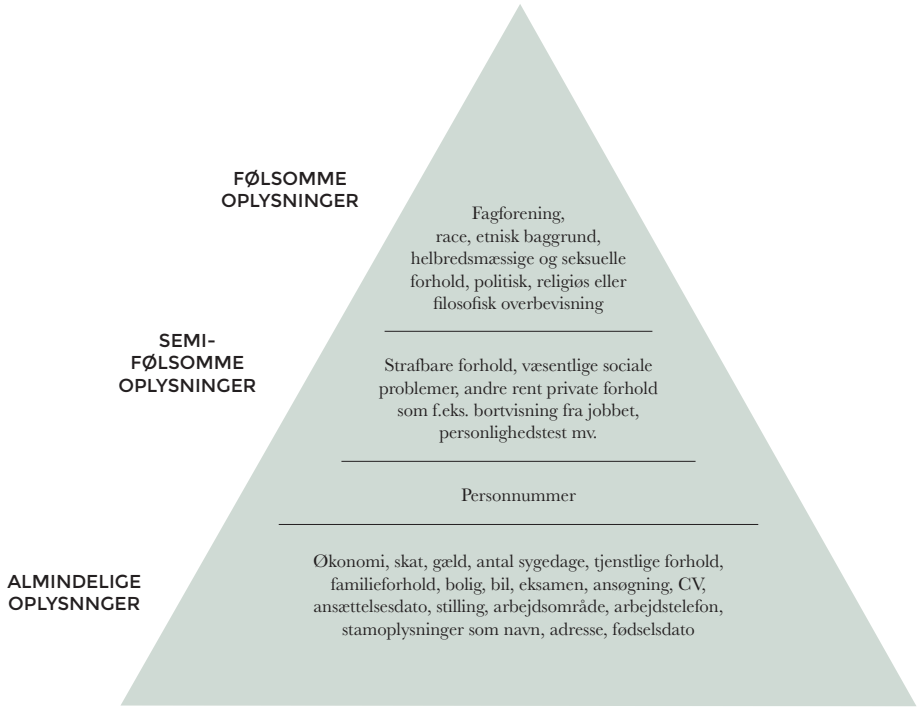
Sker behandlingen med henvisning til hjemmelsbestemmelser i lovgivningen, vil der stadig skulle ske information til den enkelte borger om hvilke oplysninger, der er tale om, jf. kravet om god databehandlingspraksis (Se afsnit 8).

Som altid skal lovens generelle principper for behandling være opfyldt, jf. afsnit 4.2. Organisationen kan således ikke sætte sig ud over kravet om saglighed, proportionalitet, mv., ved at få et samtykke til en behandling af en oplysning fra en kunde.

Reglerne fra 25. maj 2018
Forordningen indeholder også muligheder for at anvende samtykke som grundlag for behandling af personoplysninger.

Indgår et samtykke i en skriftlig erklæring med andre forhold, skal anmodningen om samtykke klart kunne skelnes fra disse andre forhold. En anmodning om samtykke skal ske i en lettilgængelig og letforståelig form. Sproget skal være klart og enkelt. Overholdes reglerne ikke, vil en sådan del af erklæringen ikke være bindende. Organisationen skal oplyse om, at samtykket kan trækkes tilbage. Tilbagetrækning skal kunne ske lige så let, som samtykket er givet. Når det skal vurderes, om samtykke er givet frit, skal der bl.a. tages størst muligt hensyn til, om opfyldelse af eksempelvis en kontrakt er gjort betinget af et samtykke til behandling af personoplysninger, som ikke er nødvendige for at opfylde kontrakten.

4.3.6 Illustration vedrørende personoplysninger i persondataloven
Persondatalovens opdeling af de forskellige kategorier af oplysninger kan illustreres på denne måde:



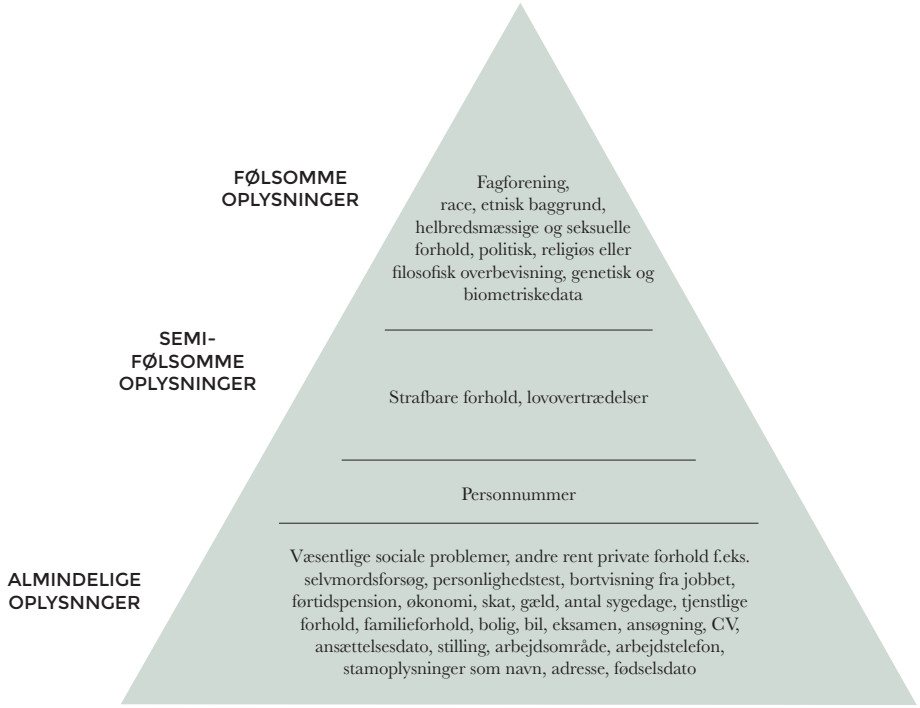
4.3.7 Reglerne fra 25. maj 2018
Der er i det nye regelsæt lagt op til, at den særlige kategori af semi-følsomme oplysninger udgår. Strafbare forhold reguleres i en særskilt bestemmelse i overensstemmelse med de gældende regler. På trods af denne ændring er det Justitsministeriets vurdering, at beskyttelsesniveauet ikke reelt sænkes. Baggrunden herfor er de skærpede krav til proportionalitetsvurderingen, som behandling af sådanne oplysninger indebærer efter regelsættes ufravigelige grundlæggende behandlingsprincipper, se afsnit 4.2.

Samtidig vil kategorien følsomme oplysninger fremover indeholde behandling af biometrisk data, der har til formål entydigt at identificere en fysisk person, f.eks. ansigtsgenkendelse eller fingeraftryk, og genetiske data. Da kategorien af semi-følsomme oplysninger udgår, vil andre rent private forhold, såsom væsentlige sociale problemer, derfor fra den 25. maj 2018 blive anset for at være almindelige oplysninger.

4.3.8 Kort om forskningsprojekter, dokumentation mv.
Behandling af oplysninger om de borgere, der er visiteret til tilbud efter serviceloven tager som udgangspunkt afsæt i, at der er tale om opsamling af oplysninger, der er relevante i forhold til det pleje-mæssige og/eller socialpædagogiske arbejde med den enkelte. Er der tale om, at en organisation af andre årsager, f.eks. ønsket om at forske i metoder eller behovet for dokumentation, ønsker at samle oplysninger, før, under eller efter et ophold, så bør det ske på baggrund af et samtykke fra den enkelte borger.

I den forbindelse kan der udarbejdes en kort samtykkeerklæring, der beskriver formålet med opsamlingen af data, hvordan det vil blive brugt, og hvornår de opsamlede data vil blive slettet.

4.3.9 Illustration vedrørende personoplysninger i persondataforordningen
Persondataforordningens opdeling af de forskellige kategorier af oplysninger kan illustreres på denne måde:



5 PERSONNUMMER

Persondataloven har særlige regler om, at behandling af personnummer kan ske, hvis det følger af lovgivningen, eller den registrerede har givet sit samtykke.

Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation af den registrerede eller som journalnummer. En organisation kan derfor registrere registreredes personnumre, hvis det er nødvendigt for at identificere personen efter særlovgivningen. Eksempelvis kan et privathospital foretage registrering af patienters personnumre på sundhedsområdet, når det fremgår af regler i sundhedsretten. En organisation må som udgangspunkt ikke videregive personnummeret til andre, medmindre særlige betingelser i loven er opfyldt.

Reglerne fra 25. maj 2018
Databeskyttelsesforordningen giver mulighed for, at personnummeret fortsat reguleres af særlige danske regler. Justitsministeriet lægger i udkastet til lovforslaget op til, at de gældende regler om personnummeret skal fortsætte. Samtidig skal private også fortsat have mulighed for at behandle personnummeret, når betingelserne for behandling af følsomme oplysninger er opfyldt.

Det betyder, at private organisationer må behandle cpr-oplysninger, når
- Det følger af lov eller lovbestemmelser fastsat i henhold til lov (f.eks. sundhedslovgivningen).
- Den registrerede har givet sit udtrykkelige samtykke.
- Der er tale om videnskabelige eller statistiske formål.
- Betingelserne for behandling af følsomme oplysninger er opfyldt.

Private organisationer må desuden videregive cpr-oplysninger, når:

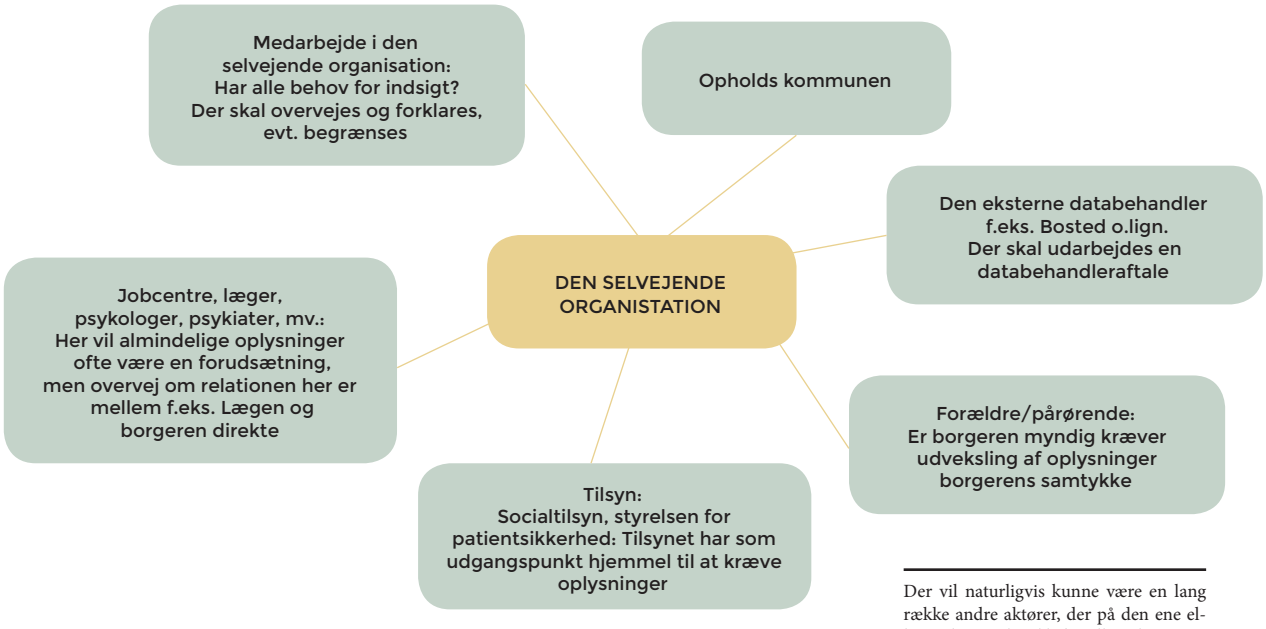
- Videregivelsen er et naturligt led i den normale drift.
- Videregivelsen er af afgørende betydning for at sikre en entydig identifikation.
- Videregivelsen kræves af en offentlig myndighed.

5.1 Hvem udveksles data med?

5.1.1 Kortlægning af organisationens omverden

Som et led i arbejdet med borgere, og i forhold til vurderingen af hvorvidt der er hjemmel til at opsamle data, vil det være afgørende, at forholde sig til hvem der er modtager af oplysninger, med andre ord hvem der vil kunne få indsigt i de oplysninger, der opsamles, med hvilken hjemmel og i hvilket omfang.

Nedenstående model viser et udsnit af de aktører, der befinder sig rundt om organisationer, der arbejder med velfærd. Modellen kan anvendes som afsæt til en kortlægning af hvilke aktører der skal indtænkes i forhold til behandling af data i den enkelte organisation.



Der vil naturligvis kunne være en lang række andre aktører, der på den ene eller anden måde vil behandle oplysninger om den enkelte borger. Det vil være centralt at forholde sig til disse og konkret vurdere hvilke datamæssigt relation, der skal være hvis nogen. Og husk altid princippet om god databehandling.

5.1.2 Tavshedspligt

Ansatte i en række selvejende organisationer er på linje med offentligt ansatte underlagt en omfattende tavshedspligt. Det fremgår af lov om retssikkerhed og administration på det sociale område § 43, der lyder:

Når en myndighed overlader opgaver efter lov om aktiv socialpolitik, lov om en aktiv beskæftigelsesindsats, dagtilbudsloven, lov om sygedagpenge, lov om ret til orlov og dagpenge ved barsel og lov om social service til andre end offentlige myndigheder, er disse omfattet af reglerne i forvaltningsloven og lov om offentlighed i forvaltningen bortset fra bestemmelserne i §§ 11-12 og 15-17 i forhold til den opgave, der udføres. Dette gælder også for privatinstitutioner, jf. § 19, stk. 5, og § 51, stk. 4, i dagtilbudsloven og for friplejeboliger.

Stk. 2. Ved opgavevaretagelsen, jf. stk. 1, er videregivelse og indhentelse af oplysninger vedrørende enkeltpersoner omfattet af forvaltningslovens §§ 27, 29, 31 og 32. Dette gælder også for selvejende institutioner, der efter aftale udfører en opgave for en kommunalbestyrelse eller et regionsråd.

Omfanget af den tavshedspligt er, som det fremgår af bestemmelsen, nærmere defineret i forvaltningsloven, og her fremgår det bl.a. af lovens § 27, at man har tavshedspligt i forhold til enkeltpersoners private, herunder økonomiske forhold, samt at videregivelse af oplysninger til en anden forvaltningsmyndighed (f.eks. den visiterende kommune) kun kan ske, hvis videregivelsen er "af betydning for myndighedens virksomhed eller for en afgørelse, som myndigheden skal træffe" (lovens § 31, stk.1).

Bestemmelsen kan begrunde, hvorfor den selvejende organisation i f.eks. statusrapporter løbende kan give den visiterende kommune eller opholdskommunen en beskrivelse af den enkelte borger og dennes aktuelle situation. Husk dog, at der kun skal gives de relevante informationer. I praksis ses det ofte, at statusrapporter gennemgås med borgeren inden de sendes til kommunen, således at borgeren gives en mulighed for at få tilføjet sine egne ord og betragtninger.

5.1.3 Kommunikation via mail eller hjemmesider

Stort set al kommunikation mellem en organisation og organisationens omverden sker i dag via e-mails eller hjemmesider, hvor oplysninger overføres direkte til f.eks. modtagerens hjemmeside. Det er også tilfældet på velfærdsområdet, hvor data om borgeren i vid udstrækning overføres fra et plejehjem, et opholdssted eller en beskæftigelsesaktør til borgerens hjemkommune, og hvor der ofte vil være tale om såvel følsomme oplysninger som almindelige oplysninger om borgerens sundhed, behandling, diagnoser, sociale forhold, mv.

Datatilsynet har forholdt sig til den kommunikation og anlægger helt overordnet en pragmatisk tilgang til området. En tilgang, der også søger at tage højde for at netop elektroniske kommunikationsformer er den måde stort set al kommunikation foregår, og derfor vil Datatilsynets vurdering af området også løbende følge med den teknologiske udvikling, med andre ord vil man som organisation skulle følge med tiden, og det er f.eks. bl.a. den tilgang, der bevirker, at der sondres mellem hjemmesider og e-mails, hvor muligheden for at sikre kryptering aktuelt er lettere i forhold til den første gruppe.

Helt overordnet skal anvendelse af elektroniske kommunikationsformer ske i overensstemmelse med god databehandlingsskik (se afsnit 4.2). I sin tilgang til området sondrer Datatilsynet mellem den kommunikation, der foregår via hjemmesider og den, der foregår via e-mail.

Kommunikation via hjemmesider

Datatilsynet stiller i forhold til kommunikation via hjemmesider (dvs. i den situation at oplysninger overføres direkte til modtagerens hjemmeside) kun udtrykkeligt krav om kryptering ved:

- Overførsel af følsomme oplysninger via hjemmesider.
- Overførsel af personnumre via hjemmesider.
- Tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med vilkår om konkrete sikkerhedsforanstaltninger ved transmission over internettet.

I en række andre situationer anbefaler Datatilsynet, at personoplysninger beskyttes, når de overføres via internettet.

Kommunikation via e-mail

Med mindre der er stillet specifikke krav om kryptering, er det som udgangspunkt op til den enkelte or-ganisation, at vurdere og beslutte hvilke sikkerhedsforanstaltninger der er nødvendige, når personoplysninger overføres ved e-mail. Af Datatilsynets vejledning fremgår følgende om den vurdering[4]:

-
- Typen af oplysninger og den sammenhæng de indgår i, herunder hvilke konsekvenser tab af oplysninger kan have.
- Om der er tale om overførsel af personoplysninger mellem:
    - To professionelle parter som f.eks. advokater, fagforeninger, revisorer mv., hvor andre personer om tales.
    - En professionel aktør og en privat person som f.eks. en kunde, en klient, et medlem mv.
- De omkostninger, som er forbundet med at iværksætte sikkerhedsforanstaltninger.

Som udgangspunkt peger tilsynet kun på følgende tre områder, hvor der ved e-mail kommunikation bør anvendes kryptering:

[4] www.datatilsynet.dk/erhverv/internettet/krav-og-anbefalinger-ifm-overfoersel-af-personoplysninger-via-internettet/

1. Når følsomme personoplysninger sendes med e-mail via internettet.
2. Når personnummer sendes med e-mail via internettet.
3. Når password og lignende sendes med e-mail via internettet.

Da der således ved anvendelse af e-mail er en højere grad af konkret vurdering, vil hensynet til god databehandlingsskik veje tungt, og her skal nævnes nogen andre foranstaltninger, der kan iagttages med henblik på at øge datasikkerheden. Det kan handle om at sikre at alle telefoner der kan modtage og opbevare e-mails er låst, at telefoner kan låses/slettes i forbindelse med bortkomst, at personfølsomme oplysninger hurtigt flyttes fra mails over i et lukket system, at mails slettes effektivt samt en klar intern politik, der understøtter ovenstående.

6 DATAANSVARLIG ELLER DATABEHANDLER?

Det er i forhold til forståelsen af det ansvar, man har, afgørende, at tage stilling til om man er dataansvarlig eller databehandler. De to roller er defineret i persondatalovens § 3, stk. 4 og 5

Stk. 4, Den dataansvarlige:
Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger.

Stk. 5, Databehandleren:
Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

Den dataansvarliges opgaver inkluderer bl.a.:

- At det som udgangspunkt er den dataansvarlige, der er ansvarlig for overholdelsen af persondataloven.
- At det er den dataansvarlige, der har pligt til at anmelde visse behandlinger af personoplysninger til Datatilsynet.
- At det er den dataansvarlige, over for hvem en registreret kan udøve sine rettigheder efter persondataloven, herunder sin indsigtsret, retten til at få berigtiget urigtige oplysninger mv.

Det er vurderingen, at langt de fleste medlemmer af Selveje Danmark vil være at betragte som dataansvarlige, da de se selv indhenter, behandler og anvender data om den enkelte borger. Samtidig vil en lang række selvejende organisationer have indgået en eller flere aftaler med eksterne leverandører af journaliseringssystemer/dagbøger, hvor den eksterne leverandør kommer til at fungere som databehandler, med hvilken der skal indgås en databehandleraftale.

Det er dog ikke sikkert, at dette udgangspunkt gælder alle. Er der tale om, at al behandling af persondata sker efter direkte instruks fra f.eks. en kommune, og anvendes data alene til det instruerede formål, vil den selvejende organisation konkret kunne blive betragtet som databehandler.

Fra Datatilsynets hjemmeside finder man følgende beskrivelse af databehandlerens håndtering af personoplysninger:
En databehandler kendetegnes altså ved kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Databehandleren behandler således aldrig personoplysninger til egne formål og må derfor ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

7 DATABESKYTTELSESRÅDGIVER

7.1 Nye regler om databeskyttelsesrådgivere

I dag indeholder den danske persondatalovgivning ikke regler om særlige databeskyttelsesrådgivere hos organisationer, mv. Sådanne regler indføres med det nye regelsæt fra 25. maj 2018.

Det danske begreb "databeskyttelsesrådgiver" svarer til det engelske "data protection officer" eller forkortet "DPO", der også i dansk sammenhæng ses anvendt flere steder. I Danmark er udpegelsen af en DPO noget nyt. Vurderingen

af, om der skal udpeges en DPO, stammer fra en af de grundlæggende regler i persondataforordningen: Ansvarlighed ("Accountability"). Efter persondataforordningen skal alle dataansvarlige og databehandlere sikre, at de har et overblik over, hvilke personoplysninger de behandler, og hvordan de behandles.

Datatilsynet har i september 2017 udsendt en vejledning om databeskyttelsesrådgivere. Reglerne kan på flere punkter give anledning til fortolkningstvivl. Hovedpunkter i regelsættet gennemgås i det følgende, men kontakt gerne Dansk Erhverv, hvis du har brug for nærmere rådgivning om reg-lerne om databeskyttelsesrådgivere.

7.2 Hvem skal have en databeskyttelsesrådgiver?

7.2.1 Offentlige myndigheder

Offentlige myndigheder og offentlige organer skal altid udpege en DPO, uanset om de er dataansvarlige eller databehandlere.

7.2.2 Private aktører på det offentlige område

Kravet om en databeskyttelsesrådgiver gælder også for ikke-offentlige aktører der fungerer som en "offentlig myndighed" eller et "offentligt organ". Disse begreber er ikke defineret direkte i forordningen.

Justitsministeriet antager, at begreberne må udfyldes af Danmark i overensstemmelse med vores traditionelle afgrænsning af det offentlige. Ministeriet henviser i den forbindelse til afgrænsningen i forvaltningslovens § 1, stk. 1-2. Her beskrives, hvordan forvaltningsloven ud over den offentlige forvaltning også gælder for:

- Al virksomhed der udøves af selvejende institutioner, foreninger, fonde m.v., der er oprettet ved lov eller i henhold til lov.
- Al virksomhed der udøves af selvejende institutioner, foreninger, fonde m.v., der er oprettet på privatretligt grundlag, og som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentligt tilsyn og intensiv offentlig kontrol (Kan være gennem driftsoverenskomst).

For så vidt angår selvejende institutioner mv. oprettet på privatretligt grundlag (forvaltningslovens § 1, stk. 2, nr. 2), vil der således efter ministeriets vurdering være nogle, som bliver omfattet af kravet om en databeskyttelsesrådgiver, mens andre ikke gør. Ministeriet tilkendegiver i øvrigt, at i det omfang særlovgivning har reguleret, at forvaltningsloven finder anvendelse for private organisationer, vil der ikke være tale om en offentlig myndighed i regelsættets forstand.

Henvisningen til forvaltningslovens definition af offentlig myndighedsudøvelse og faktisk forvaltnings-virksomhed betyder, at eksempelvis private aktører på det offentlige område som selvejende institutioner, foreninger, fonde, m.v., der er oprettet på privatretligt grundlag, således vil kunne være omfattet som offentlig myndighed, hvis de udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, tilsyn og kontrol, det kan være gennem en driftsoverenskomst. Vurderes det, at eksempelvis en selvejende institution ikke er omfattet som offentlig myndighed, vil institutionen fortsat skulle vurdere, om man er omfattet af kravet om en DPO som privat virksomhed.

7.2.3 Private organisationer

For private organisationer indføres der krav om at udpege en DPO i visse tilfælde. Private organisationer der opfylder tre betingelser skal udpege en DPO. Forpligtelsen gælder både for dataansvarlige og databehandlere, hvis betingelserne er opfyldt.

Med til at sikre ansvarlighed efter persondataforordningen er således også at foretage selve vurderingen af, om organisationen har behov for at udpege en DPO, der understøtter, at behandlingen af personoplysninger sker korrekt, uanset om man når frem til, at man skal have en DPO eller ej. Kort fortalt skal en organisation have en DPO, hvis:

- Organisationens kerneaktivitet er behandling af personoplysninger
- Der sker behandling af personoplysninger i et stort omfang
- Behandlingen er regelmæssig og systematisk overvågning af personer eller behandlingen omfatter følsomme oplysninger eller oplysninger om strafbare forhold.

Alle tre betingelser skal være opfyldt, og opfylder organisationen eksempelvis kun to af betingelserne, vil organisationen ikke være forpligtet til at udpege en DPO.

1. Betingelse
Hvad er omfattet af begrebet "kerneaktivitet"?

Begrebet kerneaktivitet kan i persondataretlig forstand være en svær størrelse at fastslå. Med til vurderingen af, om organisationer behandler personoplysninger som deres kerneaktivitet, skal tages det faktum, om behandlingen af personoplysninger er organisationens hovedaktivitet. Behandling af medarbejderes personoplysninger i HR-regi som eksempelvis ansættelseskontrakter, medarbejderudviklings-samtaler og medarbejdermapper, samt personoplysninger, som behandles på organisationens kunder til brug for kundekontakt, salg og support, vil ikke være organisationens hovedaktivitet.

Derimod vil der være tale om en organisations kerneaktivitet, hvis der i organisationens produkt eller tjenesteydelse direkte er tale om behandling af personoplysninger, eller produktet eller tjenesteydelsen er knyttet til behandlingen af personoplysninger, fordi produktet eller tjenesteydelsen ellers ikke kan leveres. Det vil eksempelvis gælde forsikringsselskaber, privathospitaler, søgemaskiner, teleselskaber, internet-udbydere, og hvis virksomheden hoster hjemmesider eller data.

2. Betingelse
Hvad menes der med behandling i "stort omfang"?

Først når der er tale om behandling af personoplysninger i stort omfang, vil betingelse nummer 2 være opfyldt. For at vurdere om der er tale om behandling i stort omfang, skal virksomheden vurdere antallet af personer, der behandles oplysninger om, mængden og typerne af personoplysninger, varigheden af behandlingen, og hvor stor geografisk udstrækning, der er tale om. Udbyder virksomheden eksempelvis kun ydelser i en bestemt mindre landsdel, vil det kunne tale for, at der ikke er tale om behandling i et stort omfang, da der er tale om en mindre geografisk udstrækning, end hvis behandlingen var i en hel landsdel, som omvendt vil kunne tale for behandling i et stort omfang.

Er der imidlertid tale om en lægepraksis, vil en mindre lægepraksis med få læger formentlig ikke behandle personoplysninger i et stort omfang, da der er tale om en begrænset mængde oplysninger på patienter, der behandles. Er der derimod tale om en stor lægepraksis, vil antallet af patienter og dermed den større mængde af personoplysninger, der behandles, tale for, at der er tale om behandling i stort omfang.

Vejledningen udsendt af Datatilsynet i september 2017 nævner, at man i vurderingen skal medtage årlig omsætning og antallet af tilknyttede læger.

3. Betingelse
Hvad er regelmæssig og systematisk overvågning af personer eller følsomme oplysninger og oplysninger om strafbare forhold?

Som betingelse nummer 3 skal virksomheden enten behandle personoplysninger i form af regelmæssig og systematisk overvågning af personer eller følsomme oplysninger og oplysninger om strafbare forhold.

Regelmæssig og systematisk overvågning af personer

Når en virksomhed sporer (tracker) eller profilerer registrerede personer på blandt andet internettet, vil der være tale om regelmæssig og systematisk overvågning af personer. Som eksempler kan nævnes profilering ved risikovurderinger såsom kreditvurderinger, vurderinger af forsikringspræmier, tracking af lokalitet via applikationer og adfærdsbaseret annoncering. Sidstnævnte udføres ofte af marketingfirmaer, som således vil kunne være omfattet af betingelsen.

Følsomme oplysninger og oplysninger om strafbare forhold

Behandling af følsomme oplysninger om en person vil være oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetisk og/eller bio-metrisk data, seksuel orientering og seksuelle forhold, og ikke mindst helbredsoplysninger. Oplysninger om strafbare forhold er oplysninger om en persons straffedomme og lovovertrædelser.

7.2.4 DPO'ens rolle i organisationen - opgaver, stilling og afskedigelsesbeskyttelse

DPO'en understøtter, at din organisation overholder reglerne i persondataforordningen. DPO'en skal inddrages i alle spørgsmål, der drejer sig om databeskyttelse og skal rådgive om reglerne herom. DPO'en bliver således en integreret

del af organisationen, og han/hun kan derfor også med fordel have andre opgaver for organisationen, så længe disse opgaver ikke fører til en interessekonflikt med rollen som DPO. Om DPO'en skal være fuldt dedikeret til sit arbejde som DPO, afhænger af omfanget af de personoplysninger, som organisationen behandler. Særligt i forhold til Datatilsynet, der fører tilsyn med, at persondatareglerne overholdes, skal DPO'en samarbejde med Datatilsynet. DPO'en fungerer således som organisationens kontaktperson ved henvendelser til og fra Datatilsynet.

Da en DPO skal være uafhængig og i stand til at udøve uvildig rådgivning til organisationen, må en DPO ikke være den øverste IT-ansvarlige eller den øverste HR-ansvarlige i organisationen. Det kan imidlertid både være en intern medarbejder, en ekstern konsulent eller en fælles DPO for hele eller flere koncernforbundne organisationer.

Kravene til DPO'ens position i organisationen afhænger af den enkelte organisation, og det er således en konkret vurdering fra organisation til organisation, hvilken løsning der vil fungere bedst.

Er du som organisation forpligtet til at udpege en DPO, skal det senest ske den 25. maj 2018, når persondataforordningen træder i kraft. Dansk Erhverv anbefaler dog, at DPO'en ansættes inden da, da det vil give DPO'en mulighed for at sætte sig ordentligt ind i organisationen og – ikke mindst – organisationens behandling af personoplysninger.

Databeskyttelsesrådgiveren må ikke afskediges eller straffes af organisationen for at udføre sine opgaver som databeskyttelsesrådgiver.

Dansk Erhverv anbefaler derfor, at man som organisation bør være særligt opmærksom på, at en frivillig udnævnelse af en databeskyttelsesrådgiver automatisk medfører, at reglerne for og forpligtelserne over for en DPO træder i kraft. Det er derfor særligt vigtigt, at man overvejer, om man har pligt til at have en DPO eller ej, og at man i den forbindelse foretager en konkret vurdering af DPO'ens rolle i organisationen og organisationens værdi af at have en DPO, selvom det ikke nødvendigvis er lovpligtigt. Som alternativ kan man overveje at udpege en compliance-rådgiver, der ikke vil være omfattet af reglerne for DPO'ere i persondataforordningen.

8 OPLYSNINGSPLIGT OG INDSIGTSRET

8.1 Organisationens oplysningspligt

Efter persondataloven skal organisationen som udgangspunkt oplyse en registreret om en række forhold, hvis organisationen indsamler oplysninger om vedkommende. Det gælder:

- Organisationens identitet.
- Formålene med behandlingen af oplysningerne.
- Yderligere oplysninger, som er nødvendige for, at vedkommende kan varetage sine interesser. Her tages hensyn til, hvordan oplysningerne er indsamlet. Det kan f.eks. være:
    - Om det er frivilligt at svare på evt. stillede spørgsmål mv.
    - Den registrerede indsigtsret i oplysningerne m.m.
    - Kategorier af modtagere af oplysningerne.
    - Hvilke oplysninger der er tale om mv. (ved indsamling hos andre end vedkommende).

Hvis den registrerede allerede kender oplysningerne, skal organisationen ikke oplyse disse forhold.

Oplysningspligten er dog ikke uden undtagelser. F.eks. har organisationen ikke en oplysningspligt, hvis den registreredes interesse i at få kendskab til oplysningerne bør vige for afgørende hensyn til private interesser. F.eks. organisationens forretningshemmeligheder. Oplysningspligten gælder alene for behandling, der sker elektronisk eller i et register, jf. afsnit 3.1.

Reglerne fra 25. maj 2018

Der vil fortsat bestå en oplysningspligt efter 25. maj 2018. Samtidig udvider databeskyttelsesforordningen området for, hvilke oplysninger en organisation skal give f.eks. en registreret, når der indsamles oplysninger om vedkommende. Dette kan beskrives i persondatapolitikken (se bilag 2).

Hvis organisationen indsamler oplysninger om den registrerede, skal organisationen oplyse følgende ved indsamlingen:
- Identitet og kontaktoplysninger.
- Hvis organisationen har en databeskyttelsesrådgiver, så kontaktoplysninger for denne. Se afsnit 5.
- Retsgrundlaget for behandlingen. Hvis organisationen behandler oplysninger efter en berettiget interesse, skal organisationen oplyse denne interesse. Se afsnit 3.3.4.
- Eventuelle modtagere eller kategorier af modtagere af oplysningerne.
- Kategorier af oplysninger (ved indsamling hos andre end den registrerede).

Samtidig skal organisationen give en række andre oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling. Justitsministeriet vurderer her, at det må afhænge af en konkret vurdering, om oplysningerne skal gives:
- Tidsrummet oplysningerne opbevares i eller, hvis ikke muligt, de kriterier, der anvendes til at fastlægge tidsrummet. Her vurderer Justitsministeriet, at en henvisning til relevante forældelsesregler kan være tilstrækkeligt.
- Ret til indsigt, berigtigelse, sletning, indsigelse, begrænsning mv.
- Ret til at trække et samtykke tilbage.
- Klagemulighed til Datatilsynet.
- Om meddelelse af oplysninger er krav efter lovgivning, en kontrakt mv.
- Hvor oplysningerne stammer fra (når indsamlingen sker hos andre end personen selv).

Der er særlige regler om overførsler til tredjelande eller internationale organisationer samt automatiserede afgørelser.

Kender den registrerede oplysningerne, skal organisationen fortsat ikke give den registrerede oplysninger om disse. Men da oplysningspligten med databeskyttelsesforordningen udvides til flere elementer, vil oplysningspligten i praksis udvides. I udkastet til databeskyttelsesloven er der lagt op til, at oplysningspligten fortsat ikke gælder, hvis bl.a. den registreredes interesse i oplysningerne bør vige for afgørende hensyn til private interesser, f.eks. forretningshemmeligheder.

Justitsministeriet planlægger at udgive en særskilt vejledning om den registreredes rettigheder, herunder oplysningspligten, i januar 2018.

Et forslag: Det bør dog overvejes, af organisationen, særligt i de situationer hvor registrering af data sker med hjemmel i lov eller lignende, at udarbejde en kort beskrivelse af hvilke typer information der opbevares, med hvilket formål og hvilke rettigheder borgeren har i forhold til de indsamlede informationer. En sådan mere generel beskrivelse kan såvel udleveres til den enkelte borger som ligge tilgængelig på f.eks. organisationens hjemmeside.

8.2 Registreredes indsigtsret

Den registrerede har som udgangspunkt ret til indsigt i de oplysninger, som organisationen behandler om vedkommende. Den registrerede kan derimod ikke kræve indsigt i oplysninger om andre personer, f.eks. pårørende.

Indsigtsretten omfatter:
- Hvilke oplysninger, der behandles.
- Behandlingens formål.
- Kategorier af modtagere af oplysningerne.
- Tilgængelig information om, hvor oplysningerne stammer fra.

Organisationen skal besvare en indsigtsbegæring snarest muligt. Er der ikke svaret inden 4 uger, skal den registrerede have oplyst hvorfor, og hvornår svaret vil foreligge. Som udgangspunkt kan indsigtsret først kræves igen 6 måneder fra den seneste meddelelse.

Organisationen kan afslå indsigtsret helt eller delvist, hvis det er afgørende af hensyn til private interesser, såsom organisationens forretningsgrundlag, forretningspraksis, knowhow eller i forbindelse med mulige retskrav. I relation til en registreret vil indsigtsret for eksempel formentlig kunne afslås eller begrænses, hvis organisationen har foretaget en

vurdering af den registrerede, eventuelt med henblik på en afgørelse eller for at gøre et muligt retskrav gældende, som den registrerede ikke skal gøres bekendt med endnu. Indsigtsretten gælder alene for behandling, der sker elektronisk eller i et register, jf. afsnit 3.1.

Reglerne fra 25. maj 2018
Den registrerede har efter forordningen som udgangspunkt adgang til de oplysninger, som organisationen behandler om vedkommende. Den registrerede har fortsat ret til information om en række forhold, hvor forordningen på visse punkter udvider organisationens informationsforpligtelser over for den registrerede. Samlet set har den registrerede ret til adgang til oplysningerne og følgende information:

- Formålet med behandlingen af oplysningerne.
- Kategorier af oplysninger.
- Eventuelle modtagere eller kategorier af modtagere af oplysningerne.
- Tidsrummet oplysningerne opbevares i eller, hvis det ikke er muligt, de kriterier, der anvendes til at fastlægge tidsrummet.
- Ret til berigtigelse, sletning, indsigelse, begrænsning mv.
- Klagemulighed til Datatilsynet.
- Hvor oplysningerne stammer fra (når indsamlingen sker hos andre end personen selv).

Der gælder særlige regler om automatiserede afgørelser samt overførsler til tredjelande eller internationale organisationer.

Det står direkte i forordningen, at organisationen (den dataansvarlige) som udgangspunkt udleverer en kopi, når der anmodes om indsigt. I den forbindelse har organisationen mulighed for at kræve et gebyr for de administrative omkostninger ved gentagne anmodninger om indsigt.

Efter forordningen vil det fortsat være muligt for Danmark at gennemføre undtagelser til indsigtsretten af hensyn til andre interesser. I tråd med dette lægger Justitsministeriet i udkastet til databeskyttelsesloven op til undtagelser fra indsigtsretten. Således har den registrerede ingen indsigtsret, hvis den registreredes interesse i oplysningerne bør vige for "afgørende hensyn til private interesser, herunder hensynet til den pågældende selv" eller en række andre nævnte interesser, f.eks. forretningshemmeligheder. Justitsministeriet planlægger at udgive en særskilt vejledning om den registreredes rettigheder, herunder indsigtsretten, i januar 2018.

9 FORTEGNELSE OVER BEHANDLING

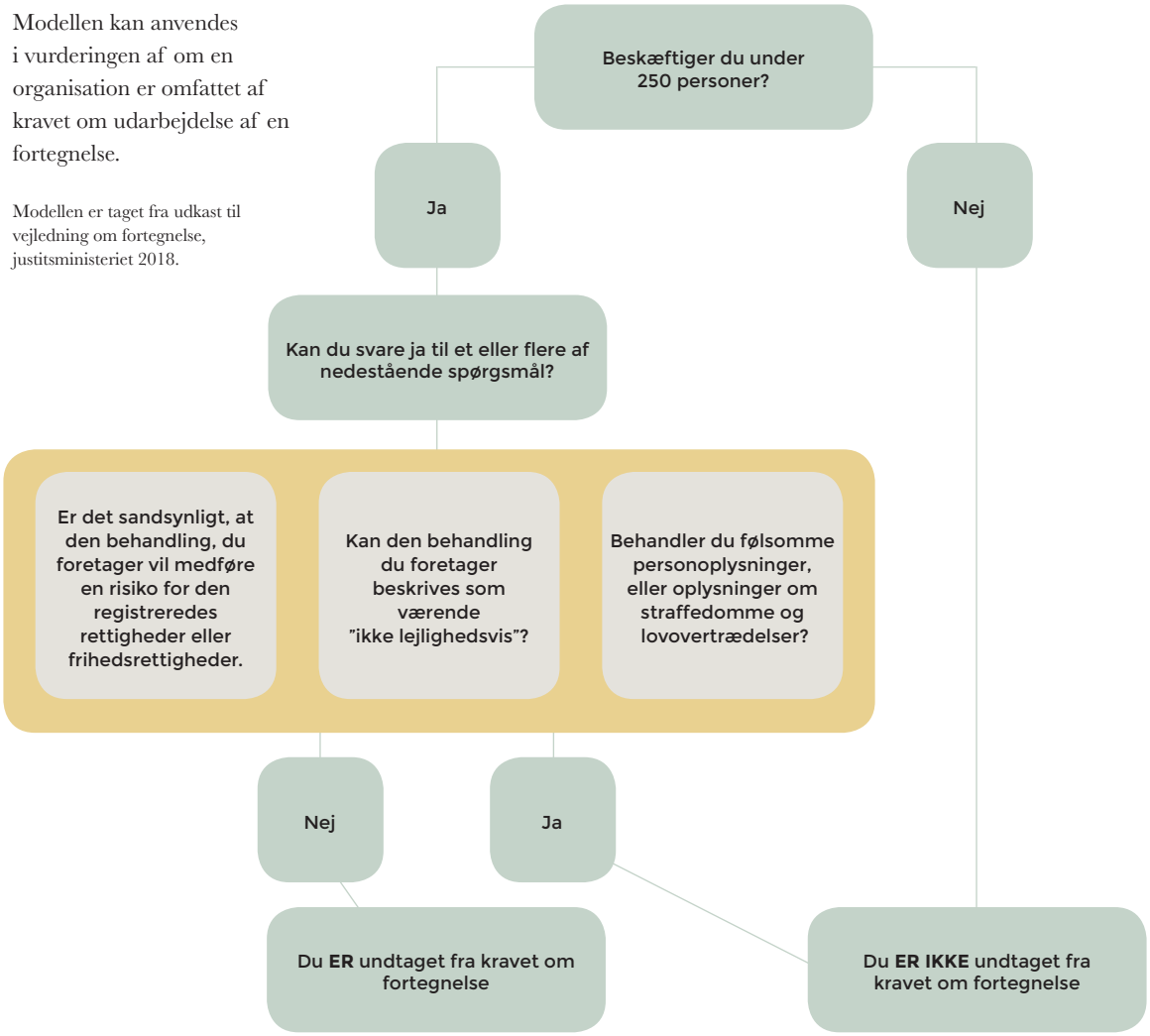
Følsomme og semi-følsomme oplysninger kan i en række tilfælde blive behandlet i forbindelse med en organisations personaleadministration. Det kan f.eks. være oplysninger om strafbare forhold, helbreds-forhold, oplysninger i forbindelse med personlighedstests eller lignende. En organisation skal efter gældende regler som udgangspunkt anmelde sådanne behandlinger til Datatilsynet. Anmeldelsen sker elektronisk via Datatilsynets hjemmeside, hvor der også findes en vejledning og en kladde til anmeldelse, www.datatilsynet.dk.

Reglerne fra 25. maj 2018
Når forordningen er trådt i kraft, skal en organisation føre en intern fortegnelse over behandlingsaktiviteter vedrørende personoplysninger under organisationens ansvar, det vil sige ikke kun personaleadministration men al behandling af personoplysninger, hvis betingelserne herfor er opfyldt. En sådan fortegnelse erstatter reglerne i dag om generel anmeldelse til Datatilsynet, jf. ovenfor.

Justitsministeriet vurderer i sin betænkning, at kravet om en fortegnelse omfatter al behandling af personoplysninger, dvs. både almindelige oplysninger, følsomme oplysninger, og oplysninger om straffedomme mv. Kravet omfatter som udgangspunkt organisationer med mere end 250 beskæftigede, men samtidig gælder kravet også de organisationer, der behandler data af mere følsom karakter, hvilket igen vil betyde, at mange organisationer på velfærdsområdet vil være omfattet af kravet, selvom de ikke har 250 beskæftigede.

Modellen kan anvendes i vurderingen af om en organisation er omfattet af kravet om udarbejdelse af en fortegnelse.

Modellen er taget fra udkast til vejledning om fortegnelse, justitsministeriet 2018.



Fortegnelsen skal som minimum indeholde:

- Kontaktoplysninger for den dataansvarlige – og hvis relevant, fælles dataansvarlig, repræsentant og databeskyttelsesrådgiver.
- Formål med behandlingen af oplysningerne (f.eks. personaleadministration)
- Kategorier af registrerede (f.eks. tidligere og nuværende patienter, beboere, borgere og kunder) og kategorier af personoplysninger (f.eks. identifikationsoplysninger, helbredsoplysninger, økonomiske forhold, sociale forhold, mv.).
- Kategorier af modtagere (herunder offentlige myndigheder, tredjelande og internationale organisationer).
- Hvis relevant, nærmere om overførsler til tredjelande og internationale organisationer.
- Hvis muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger. Ellers forventede slettefrister.
- Hvis muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger.

Fortegnelsen skal være skriftlig og elektronisk. Det er således ikke tilstrækkeligt at have en manuel fortegnelse efter forordningen.

Justitsministeriet antager, at en organisation (dataansvarlig) vil kunne føre en fortegnelse over forskellige formål, f.eks. behandling af følsomme oplysninger på patienter, personaleadministration og whist-leblowerordninger i lighed med eksempler fra Datatilsynets fortegnelser, som anvendes ved anmeldelse efter den gældende persondatalov. Har en organisation i dag anmeldt sin personaleadministration, vurderer ministeriet altså, at organisationen vil kunne genanvende

den anmeldelse, som organisationen har indsendt til Datatilsynet. Organisationen skal stille fortegnelsen til rådighed for Datatilsynet, hvis tilsynet beder om at se denne.

Se et eksempel på en fortegnelse i bilag 1.

10 OPBEVARING AF OPLYSNINGER FØR, UNDER OG EFTER BEHANLINGEN

Generelt må organisationen ikke opbevare oplysninger i længere tid end nødvendigt ud fra de formål, som oplysningerne behandles ud fra. Det gælder alle kategorier af oplysninger. Organisationen skal også have en saglig grund til opbevaringen. Se også om de generelle principper for behandling af oplysninger i afsnit 4.2.

Der er ikke fastsat en konkret tidsbegrænsning i persondataloven. Der er således overladt et skøn til organisationen, der har indhentet/registreret oplysningerne om den registrerede, hvorefter organisationen skal begrunde, at der er et sagligt formål med fortsat opbevaring af personoplysningerne. Vurderingen kan afhænge af anden lovgivning, f.eks. fristerne i forældelseslovgivningen og bogførings-lovens frister på 5 år fra relevant regnskabsår, eller specifikke frister i sundhedslovgivningen for eksem-pelvis opbevaring af patientjournaler.

Et eksempel: bekendtgørelse om patientjournaler indeholder f.eks. en række bestemmelser om hvor længe oplysninger skal gemmes, det omfatter også de "patientjournaler" der under andre navne, men med hjemmel i sundheds-lovgivningen føres af andre behandlingstilbud:

§ 15. Læger, tandlæger, kiropraktorer, jordemødre, kliniske diætister, kliniske tandteknikere og tandplejere skal opbevare deres patientjournaler i mindst 10 år (opbevaringsperioden), jf. dog stk. 5.

Stk. 2. Andre autoriserede sundhedspersoner end de af stk. 1 omfattede, skal opbevare deres patientjournaler i mindst 5 år (opbevaringsperioden), jf. dog stk. 5 og 6.

Stk. 3. Opbevaringsperioden løber fra den seneste optegnelse i patientjournalen.

Stk. 4. Opbevaringsperioden gælder, selv om patienten måtte være afgået ved døden.

Stk. 5. Patientjournaler af betydning for en klage-, tilsyns-, eller erstatningssag skal opbevares, så længe vedkommende sag verserer efter opbevaringsperiodens udløb.

Stk. 6. Hvis optegnelser foretaget af faggrupper omfattet af stk. 2, er en del af en fælles tværfaglig elektronisk patientjournal, der også omfatter faggrupper efter stk. 1, skal optegnelserne opbevares i mindst 10 år.

Stk. 7. Opbevaringsperioden gælder fortsat, selv om en autoriserede sundhedsperson er ophørt med at drive praksis, herunder fordi pågældende er død, er gået konkurs eller har overdraget sin praksis til en anden autorise-ret sundhedsperson inden for samme faggruppe til fortsat drift, jf. dog § 16, stk. 2.

I forbindelse med den generelle information af borgeren om hvilke oplysninger, der opsamles, vil det tillige være relevant at informere borgeren om, hvor længe oplysninger bevares, og hvad der efter dette tidspunkt sker med den opsamlede data.

Reglerne fra 25. maj 2018
Justitsministeriet vurderer, at indholdet af databeskyttelsesforordningens regler om opbevaring svarer til de gældende regler i persondataloven.

11 DATASIKKERHED

Persondataloven fastslår, at en organisation som dataansvarlig skal træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

- Hændeligt eller ulovligt tilintetgøres, fortabes eller forringes.
- Kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Disse regler om datasikkerhed gælder også i forhold til personoplysninger, som organisationen behandler om registrerede personer.

Datatilsynet har i den forbindelse oplistet en række specifikke minimumskrav for sikkerhed i forbindelse med behandling af personoplysninger. Datatilsynets it-sikkerhedstekster fokuserer på udvalgte it-sikkerhedsmæssige problemstillinger, som dataansvarlige, databehandlere, projektansvarlige og andre i praksis skal håndtere i forbindelse med behandling af personoplysninger.
Datatilsynets aktuelle minimumskrav kan ses her: www.datatilsynet.dk/vejledninger/it-sikkerhedstekster/.

Vurderingen af, hvilke sikkerhedskrav en organisation skal overholde i forbindelse med behandling af personoplysninger, kan ændre sig løbende over tid, bl.a. i takt med hvilke muligheder den teknologiske udvikling faktisk giver for at beskytte personoplysninger.

Reglerne fra 25. maj 2018
Kravet om, at behandling af personoplysninger skal ske med tilstrækkelig sikkerhed, er også en del af databeskyttelsesforordningen. Det er præciseret, at organisationen ud fra nedenstående punkter skal gennemføre tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau:

- Aktuelle tekniske niveau.
- Implementeringsomkostninger.
- Behandlingens karakter, omfang, sammenhæng og formål.
- Risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Forordningen indeholder også en række eksempler mv.

Ud over de særlige regler om sikkerhed, er sikkerhed også skrevet ind i forbindelse med forordningens grundlæggende principper. Justitsministeriet vurderer ikke umiddelbart, at denne præcisering i sig selv fastlægger selvstændige krav til datasikkerheden, men at den skal ses som et signal om, at sikkerheden skal tillægges stor betydning ved behandling af personoplysninger.

12 BRUD PÅ DATASIKKERHED

Selvom den enkelte organisation har gjort hvad den kunne for at skabe en høj grad af datasikkerhed, så kan det ikke udelukkes, at der sker sikkerhedsbrud. Det kan både handle om situationer, hvor nogen får adgang til nogen af de data, der ligger elektronisk, hvis data ved en fejl slettes eller på anden måde mistes, eller hvis der f.eks. sker et tyveri af en computer eller lignende.

I en situation hvor der sker et sikkerhedsbrud, vil der efter de nye regler gælde en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde bruddet til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet[5]. Samtidig fastsættes der en forpligtelse, som allerede i dag tolkes ud af persondatalovens grundregel om god databehandlingsskik og Datatilsynets praksis, til som udgangspunkt at underrette de registrerede i tilfælde af brud på persondata-sikkerheden.

Afmeldelsen til Datatilsynet kan (når den tekniske løsning er på plads) ske via Virk.dk.
Anmeldelsen til Datatilsynet skal ske, hvis bruddet indebærer en sandsynlig risiko for fysiske personers rettigheder, og her er tale om en konkret specifik vurdering, der både vil skulle inddrage omfang, betydning, informationernes karakter mv.

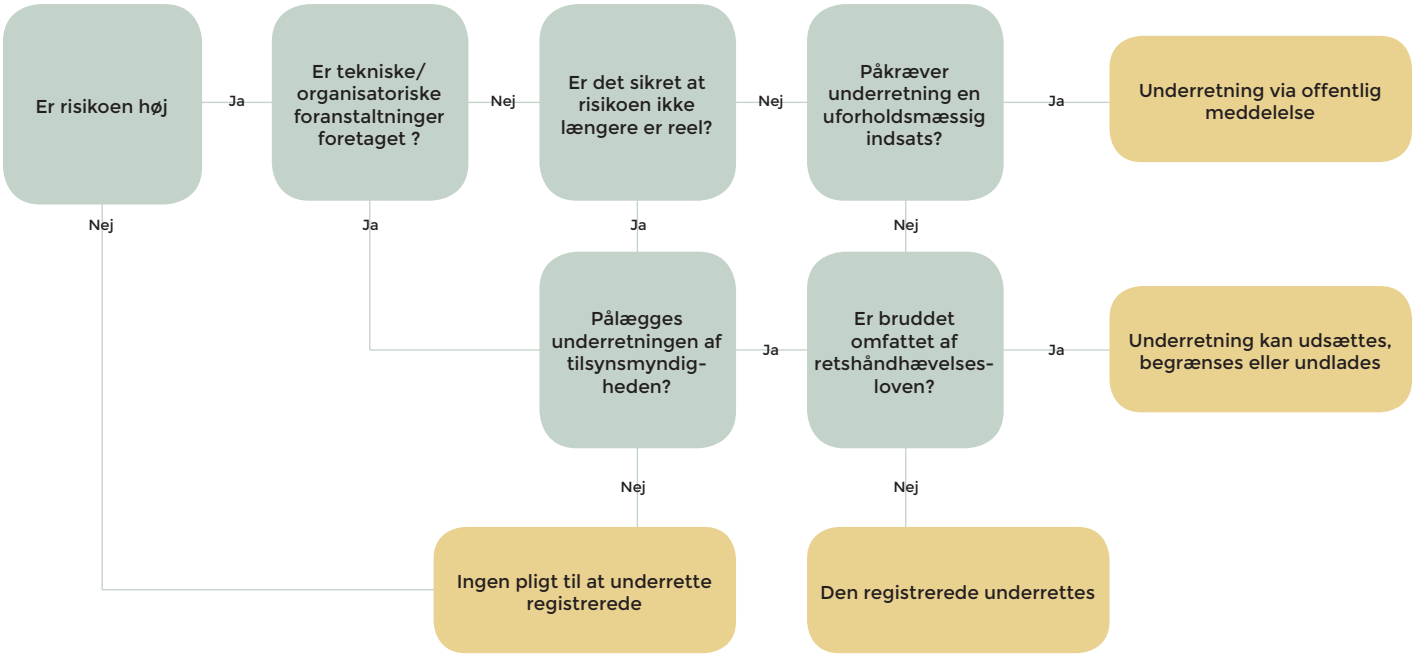
[5] www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Vurderes det, at der ikke er en sådan risiko i tilknytning til bruddet, skal den enkelte organisation lave en intern dokumentation af bruddet. En dokumentation, som det anbefales at man opbevare sammen med sin fortegnelse og andre dokumenter, der kan være af betydning, i forbindelse med et eventuelt besøg af Datatilsynet.

12.1 Skal der også ske underretning af de registrerede?

I tilfælde af brud på datasikkerheden vil der som nævnt ovenfor også i visse tilfælde skulle ske underretning af de registrerede, der kan være påvirket af bruddet. Det gælder naturligvis særligt i de tilfælde, hvor bruddet kan have konsekvenser for den enkelte f.eks. hacking af oplysninger om passwords, CPR-numre, konti mv. eller hvor oplysningerne er af en særlig følsom karakter.

Datatilsynet har i sin vejledning om håndtering af brud på persondatasikkerheden fra februar 2018 udarbejdet nedenstående model, der beskriver om og i givet fald hvordan der kan ske underretning.



I forhold til selvejende organisationer, der arbejder med velfærd, vil en række af de informationer, som opbevares om den enkelte borger, være betragtet som følsomme. Af den grund kan det også anbefales, at den enkelte organisation allerede i forbindelse med udarbejdelsen af sin fortegnelse (se bilag 1) indføjer et afsnit, der beskriver, hvordan man vil takle et eventuelt brud – både i forhold til Datatilsynet og de en-kelte borgere.

13 SANKTIONER

En person, der har lidt materiel eller immateriel skade som følge af en ulovlig behandling af personoplysninger mv., kan kræve erstatning. Overtrædelse af en række bestemmelser i persondataloven kan også medføre straf i form af fængsel eller bøde.

Reglerne fra 25. maj 2018
Som udgangspunkt vil sanktionsmulighederne ved organisationens overtrædelse af en række bestemmelser i databeskyttelsesforordningen eller databeskyttelsesloven svare til gældende ret, dog er bødestørrelserne i persondataforordningen betragtelige. Med persondataforordningens ikrafttræden er der udsigt til større sanktioner med bøder på op til 20 mio. euro eller 4 % af en organisations årlige globale omsætning på koncernniveau, hvis grundlæggende behandlingsregler ikke overholdes.

Det er således værd at hæfte sig ved, at det af bemærkningerne til udkastet til databeskyttelsesloven fremgår, at Justitsministeriet finder, at:

- Bødeniveauet bør forhøjes i forhold til det nuværende niveau efter persondataloven.
- Der vil være grundlag for, at straffen stiger i en række tilfælde.

På nuværende tidspunkt er det dog vanskeligt at sige noget om, hvordan konkrete typer af overtrædelser af reglerne for behandling af oplysninger vil blive vurderet i disse sammenhænge. En politisk stillingtagen til sanktionsspørgsmålet for offentlige myndigheder udestår i udkastet til data-beskyttelsesloven. Dog er der udsigt til fokus på øget sanktionering af offentlige myndigheder, herunder sanktionering i form af bøder.

14 ØVRIGE ELEMENTER I DET NYE REGELSÆT OM DATABESKYTTELSE

Databeskyttelsesforordningen mv. omfatter også en række andre regler, der kan have direkte eller indirekte betydning for organisationer, der behandler personoplysninger om registrerede, mv. Herunder regler om:

- Regelsættets geografiske område.
- Koncerner.
- Datatilsynet mv., herunder det europæiske samarbejde i Det europæiske Databeskyttelsesråd.
- Internationale dataoverførsler.
- Databeskyttelse by design og default.
- Konsekvensanalyser.
- Automatiserede afgørelser.
- Adfærdskodekser og certificering.

Kontakt Dansk Erhverv, hvis I har behov for særlig rådgivning om sådanne elementer i forbindelse med behandling af persondata om registrerede.

15 VIL DU VIDE MERE?

Medlemmer af Selveje Danmark og Dansk Erhverv kan kontakte Hotline i Dansk Erhverv vedrørende spørgsmål om behandling af personoplysninger på tlf. 3374 6400, eller Selveje Danmark på kontakt@selveje.dk.

Dansk Erhverv har desuden udarbejdet paradigmer for sine medlemmer knyttet bl.a. til databehandleraftaler og persondatapolitik. Desuden vil der løbende blive udarbejdet yderligere relevant materiale se www.danskerhverv.dk.

Dansk Erhverv har udgivet en række pjecer i "Gode Råd Om"-serien, der bl.a. omfatter følgende HR-områder:

- Gode råd om internet og mail
- Gode råd om sociale medier
- Gode råd om rekruttering

"Gode Råd Om"- serien findes på www.danskerhverv.dk.

Dansk Erhverv har desuden udgivet en vejledning om persondatabeskyttelse for medarbejdere.
Læs mere i Håndtering af persondata ved personaleadministration mv. på www.danskerhverv.dk.

BILAG 1 – FORTEGNELSE

Eksempel på en fortegnelse over databehandlingsaktiviteter (dataansvarlig)

Dataansvarlig	**Organisationens navn, CVR-nr. og kontaktoplysninger** (adresse, hjemmeside, telefonnummer og e-mail)	Den Selvejende Organisation NN Adresse: CVR:
	Den fælles dataansvarlige samt dennes kontaktoplysninger (adresse, hjemmeside, telefonnummer og e-mail)	Den ansvarlige for behandling af data i organisationen. Kan være forstanderen, direktøren eller en anden (f.eks. en DPO)
	Den fælles dataansvarlige samt dennes kontaktoplysninger (adresse, hjemmeside, telefonnummer og e-mail)	(Forudsætter at man skal have en DPO) Hvis ikke kan følgende tekst indføjes: *Organisationen er ikke omfattet af kravet om udpegning af en DPO.*
Formål (-ene)	**Behandlingens eller behandlingernes formål** (et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige)	F.eks.: A - Løbende beskrivelse af de indskrevne borgere, deres diagnoser, familiemæssige forhold, interesser og udvikling. B - Løbende opdatering af patientjournaler (evt. kronologisk og let overskueligt indarbejdet i dagbogen). C - Personaleadministration.
Kategorierne af registrerede og kategorierne af person-oplysningerne	**Kategori af registrerede personer** (eksempelvis borger/kunder, partsrepræsen-tanter nuværende eller tidligere ansatte, andre virksomheder, andre myndigheder mv.)	Der behandles oplysninger om følgende kategorier af registrerede personer: a) Borger, der er visiteret til organisationen. b) Pårørende c) Ansøgere d) Ansatte e) Tidligere ansatte osv.

Kategorierne af registrerede og kategorierne af person-oplysningerne	**Oplysninger, som behandles om de registrerede personer** (afkryds og beskriv de typer af oplysninger, som er omfattet af behandlingsaktiviteterne) a) Borger, der er visiteret til organisationen. b) Pårørende c) Ansøgere d) Ansatte e) Tidligere ansatte (Dette er blot et eksempel)	Oplysninger, som indgår i den specifikke behandling. Beskriv:	Person-gruppe
		Sociale forhold og kompetencer	A
		Diagnoser f.eks. ADHD, Aspergers syndrom, udviklingsforstyrelser mv.	A
		Oplysninger om uddan-nelsesaktiviteter og/eller beskæftigelse.	A
		Oplysninger om seksuelt orientering hvis relevant af sundheds-mæssige årsager.	A
		Navn og adresse samt tilhørsforhold.	B
		Identifikations-oplysninger	C
		Oplysninger vedrørende ansættelsesforholdet til brug for administration, herunder stilling og tjenestested, lønforhold, oplysninger af relevans for lønindeholdelse, personalepapirer, ud-dannelse og sygefravær.	D
		OSV.	

Modtagerne af personoplysningerne	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til.** (eksempelvis andre myndigheder, virksomheder, borger/kunder mv.)	For eksempel: 1. Offentlige myndigheder (så vidt muligt myndighedens navn, f.eks. visiterende kommuner) 2. Tilsyn (Socialtilsyn, kommunalt tilsyn, Styrelsen for patientsikkerhed) 3. Skoler, misbrugsbehandling, rehabiliteringsteams mv.
Sletning	**Tidspunkt for sletning af oplysninger** (de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger)	Oplysninger om borgere slettes senest 5 år efter borgerens fraflytning, afsluttet forløb, dødsfald. Oplysninger i patientjournaler slettes 5 år efter borgerens fraflytning, afsluttet forløb, dødsfald. Oplysninger om pårørende slettes samtidig med oplysninger om borgeren Oplysninger om tidligere ansatte slettes senest X år efter afslutningen af den journalperiode, hvor personalesagen er afsluttet. Oplysninger om ansøgere slettes senest X måneder efter afslutningen af den journalperiode, hvor sagen er afsluttet. Oplysninger overføres løbende til Rigsarkivet efter arkivlovens regler og Statens Arkivers bestemmelser herom.
Tekniske og organisatoriske sikkerhedsforanstaltninger	**Beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger** (hvis muligt skal der gives en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, jf. artikel 32, stk. 1) I tilknytning til dette punkt, kan der tillige laves en kortere beskrivelse af, hvordan organisationen til takle even-	Behandling af personoplysninger om borgeren sker i XX system, og iht. interne retningslinjer, der blandt andet indebærer, at den enkelte medarbejder alene har adgang til de oplysninger der er relevante i forhold til medarbejderens arbejde. Behandling af oplysninger om medicin, sygdom o.lign. indføres i patientjournalen, som er knyttet til XX system.

Tekniske og organisatoriske sikkerheds-foranstaltninger	tuelle brud på datasikkerheden – både i forhold til Datatilsynet og i forhold til de eventuelt berørte borgere (se ovenfor afsnit 12)	Behandling af personoplysninger i forbindelse med HR-arbejde sker i overensstemmelse med interne retningslinjer, som bl.a. fastsætter rammerne for autorisation- og adgangsstyring og logning. Personoplysninger opbevares i pseudonymiseret og i kryptret form og transmitteres krypteret. Fysisk materiale opbevares altid aflåst.

Bilag 1 er hentet i vejledning om fortegnelse, Justitsministeriet 2018. I skemaet er udtaget de elementer der handler om internationale relationer da det vurderes, at de færreste selvejende organisationer har sådanne. Men er det omvendt situationen, f.eks. hvis data opbevares i udlandet så bør det inddrages i fortegnelsen. Der henvises her til Datatilsynets egen vejledning.

BILAG 2 – SKABELON FOR PERSONDATAPOLITIK

Nærværende skabelon kan anvendes til udformning af organisationens persondatapolitik. Det kan overvejes at udarbejde én persondatapolitik i forhold til de borgere I arbejder med samt én for medarbejderforhold. I forhold til begge versioner vil de skulle være tilgængelige for de berørte grupper. Det kan anbefales at have dem på jeres hjemmeside, samt at gøre det til en fast praksis at udlevere den til borgere i forbindelse med visitation eller lignende. Der bør være en klar sammenhæng mellem persondatapolitikken og fortegnelsen (bilag1).

Persondatapolitik for
[indsæt organisationens navn]
Her kan du læse, hvordan [indsæt organisationens navn] håndtere personoplysninger.

Dataansvarlig
[indsæt firmanavn] er dataansvarlig, og vi sørger for at behandling af dine personoplysninger sker i overensstemmelse med lovgivningen.

Vores kontaktoplysninger er
[indsæt kontaktoplysninger]

Databeskyttelsesrådgiver
[Udfyldes kun hvis virksomheden har udpeget en databeskyttelsesrådgiver]
[indsæt kontaktoplysninger]

Vi behandler følgende persondata
[opdel i emner efter, hvor organisationen behandler personoplysninger, eller lav for at styrke den direkte kommunikation en persondatapolitik målrettet borgeren og en anden målrettet ansatte, ansøgere mv. Nedenfor er eksempler på former for behandling, der kan beskrives. I kan selv tilføje flere]
Når du er indskrivet hos os indsamler, vi følgende personoplysninger:
[udfyld, hvis relevant]

- List de typer af personoplysninger, der indsamles (alm./særlige kategorier).
- Formål med behandling og retsgrundlag (Her må I konkret og kort beskrive hvorfor I behandler de pågældende oplysninger, og med hvilken hjemmel, hvilket f.eks. kan være reglerne om pati-entjournaler, lov om socialtilsyn, mv.).
- Evt. modtagere af oplysninger (tilsynsmyndigheder, visiterende kommune mv.).
- Tidsrum for opbevaring, eller hvilke kriterier der anvendes til at fastlægge tidsrum (det kan f.eks. følge af hjemmelsloven, at der også er krav om, hvor længe oplysninger skal gemmes).
- Du har ret til at få dine egne personoplysninger med i et maskinlæsbart format (dataportabilitet).

Hvis du ansøger om et job hos os behandles følgende personoplysninger:

- List de typer af personoplysninger, der indsamles (alm./særlige kategorier)
- Formål med behandling og retsgrundlag
- Evt. modtagere af oplysninger
- Tidsrum for opbevaring, eller hvilke kriterier der anvendes til at fastlægge tidsrum
- Du har ret til at få dine egne personoplysninger med i et maskinlæsbart format (dataportabilitet)

Dine rettigheder

- Du har ret til at få indsigt i, hvilke personoplysninger vi behandler om dig.
- Du har ret til at få berigtiget og ajourført de personoplysninger, vi har registreret om dig.
- Du har ret til at få slettet de personoplysninger vi har registreret om dig. Ønsker du at få slettet dine personoplysninger, sletter vi alle oplysninger, som vi ikke efter lovgivning er pålagt at skulle gemme.
- Er behandlingen af personoplysninger baseret på et samtykke fra dig, har du ret til at trække samtykket tilbage, hvilket betyder, at behandling herefter ophører, medmindre vi efter lovgiv-ning er pålagt at skulle behandle personoplysningerne.

Konsekvens af tilbagetrækning af samtykke
I det omfang behandling af data er baseret på samtykke, vil en tilbagetrækning af dette kunne have konsekvenser for det videre samarbejde mellem dig og [organisationens navn].

Sikkerhed
Beskriv virksomhedens sikkerhedsforanstaltninger vedrørende behandling af personoplysninger (det kan være en beskrivelse af at kun få har adgang til data, at følsomme oplysninger krypteres når det sendes, at journaler mv. opbevares aflåst mv.)

Klageinstans
Du har mulighed for klager over vores behandling af personoplysninger om dig til Datatilsynet. Se kontaktoplysninger og mere om klageadgang her: www.datatilsynet.dk

SELVEJE DANMARK
SLOTSHOLMSGADE 1
BØRSEN
1217 KØBENHAVN K

T. 3374 6427
KONTAKT@SELVEJE.DK

WWW.SELVEJE.DK